

Valstybinė duomenų apsaugos inspekcija
prie Valdymo reformų ir savivaldybių reikalų ministerijos

Duomenų apsaugos reikalavimų nustatymo metodika

(sutrumpinta redakcija)

Vilnius • 1999

Turinys

[Pratarmė](#)

[Pagrindinių santrumpų žodynėlis](#)

[1. Rizikos veiksniai](#)

[1.1. Atsitiktinės objektyvios aplinkybės](#)

[1.1.1. Pasekmės](#)

[1.1.2. Vidiniai rizikos veiksniai](#)

Rekomenduojamos priemonės

[1.1.3. Išoriniai rizikos veiksniai](#)

Rekomenduojamos priemonės

[1.2. Netyčinės subjektyvios aplinkybės](#)

[1.2.1. Pasekmės](#)

[1.2.2. Veiksniai, kylantys dėl darbo organizavimo](#)

[nesklandumu](#)

Rekomenduojamos priemonės

[1.2.3. Veiksniai, susiję su techninės ir programinės](#)

[įrangos gedimu](#)

Rekomenduojamos priemonės

[1.2.4. Veiksniai, kylantys dėl darbuotojų klaidų](#)

Rekomenduojamos priemonės

[1.3. Tyčinės subjektyvios aplinkybės](#)

[1.3.1. Pasekmės](#)

[1.3.2. Veiksniai, kylantys dėl tyčinių
subjektyvių aplinkybių](#)

Rekomenduojamos priemonės

[2. Duomenų apsaugos priemonių aprašymas](#)

[2.1. Infrastruktūrinės priemonės](#)

[2.1.1. Pastatai](#)

[2.1.2. Techninė įranga](#)

[2.2. Administracinės priemonės](#)

[2.2.1. Darbo organizavimas](#)

[2.2.2. Personalas](#)

[2.2.3. Netikėtumų planavimas](#)

[2.3. Techninės ir programinės priemonės](#)

[2.3.1. Techninė įranga](#)

[2.3.2. Programinė įranga](#)

[2.4. Telekomunikacinės priemonės](#)

[2.4.1. Techninė įranga](#)

[2.4.2. Programinė įranga](#)

Pratarmė [Atgal į turinį](#)

Ši metodika skiriama duomenų valdytojų, jų duomenų tvarkymo įstaigų ir taip pat kitų duomenų naudotojų informacinių sistemų duomenų apsaugos reikalavimų nustatymui. Ji padės parinkti ir įdiegti duomenų apsaugos priemones, adekvačias duomenų reikšmingumo lygiui bei galimiems jų pažeidimo padariniams. Duomenų apsaugos metodika suskirstyta į du pagrindinius sąrašus – Rizikos veiksmų ir Apsaugos priemonių.

Pagrindinių santrumpų žodynėlis [Atgal į turinį](#)

ARP (Address Resolution Protocol) – adreso rezoliucijos protokolas
CMOS (Complementary Metal Oxide Semiconductor) – papildomas metalo oksido puslaidininkis

DISA (Direct Inward System Access) – tiesioginė vidinės sistemos kryptis

ICMP (Internet Control Message Protocol) – Internet tinklo valdymo pranešimų protokolas

IP (Internet Protocol) – tarptinklinis protokolas

IS – informacinė sistema

NCP (Netware Core Protocol) – NetWare tinklo branduolio protokolas

NFS (Network File System) – tinklo bylų sistema

NIS (Network Information Service) – tinklo informacinė tarnyba

OSPF (Open Shortest Path First) – trumpiausio atviro kelio pirmenybė (perdavimo protokolas)

PBX (Private Branch Exchange) – vietinis telefoninio ryšio skirstytuvus

RAM (Random Access Memory) – operatyviosios atminties įrenginys (arba laisvosios krypties atmintis)

RAS (Remote Access Service) – tolimosios krypties tarnyba

RIP (Routing Information Protocol) – maršruto informacijos protokolas
UPS (Uninterrupted Power Supply) – nepertraukiamos energijos tiekimas
UUCP (UNIX-UNIX) – kopijavimas iš vienos UNIX operacinės sistemos į kitą UNIX
WfW (Windows for Workgroups) – Windows, skirti darbinėms grupėms (tinklinė Windows versija)

1. Rizikos veiksniai [Atgal į turinį](#)

1.1. Atsitiktinės objektyvios aplinkybės [Atgal į turinį](#)

1.1.1. Pasekmės [Atgal į turinį](#)

Duomenų pažeidimo poveikio laipsnis yra labai didelis. Pagrindiniai padariniai: visos atsarginės kopijos sugadintos, ypatingai, jei jos saugomos viename pastate; sugadinta visa techninė kompiuterinė ir komunikacinė bazė; duomenys visiškai sugadinti; neveikia kompiuterinė sistema.

1.1.2. Vidiniai rizikos veiksniai [Atgal į turinį](#)

Darbuotojų praradimas. IS aptarnaujančių darbuotojų netenkama dėl ligų, nelaimingų atsitikimų, mirčių arba socialinių veiksnių įtakos, taip pat derėtų atkreipti dėmesį į darbo sutarčių galiojimo laiką.

Atsitiktinės techninės avarijos. Sugedus vienai sudedamajai daliai, gali sutrikti visos sistemos darbas. Tai taikoma centrinėms IS dalims, tokioms kaip energijos šaltiniai, vėsinimo sistemos, vietinio tinklo serveriai, duomenų perdavimo įrenginiai. Labiausiai pakenkia atsitiktiniai incidentai.

Temperatūros ir drėgmės pakitimų poveikis. Kiekvienas įtaisas turi leistiną darbo temperatūros svyravimų skalę. Dėl stiprių pokyčių galimi gedimai, darbo sutrikimai.

Purvo, dulkių bei magnetinių laukų įtaka. Į kompiuterinę ir organizacinę techniką patenka purvas, įtaisai turi būti valomi, taisomi. Todėl neišvengiamos prastovos, piniginės išlaidos. Magnetinės laikmenos yra jautrios magnetiniams laukams, todėl turėtų būti laikomos atokiau nuo elektros ar radiacijos šaltinių.

Rekomenduojamos priemonės. [Atgal į turinį](#)

Infrastruktūrinės: pastatai (patalpų išdėstymas, oro vėsinimo ir drenažo sistemos).
Administracinės: darbo organizavimas (duomenų laikmenos), personalas (darbo aplinkos gerinimas, darbo vietų užpildymas), netikėtumų planavimas (“Pavojaus” situacija, IS atsarginių dalių įsigijimo planavimas).

Techninės ir programinės: programinė įranga (duomenų laikmenų priežiūra).

Telekomunikacinės: techninė įranga (kabeliai).

1.1.3. Išoriniai rizikos veiksniai [Atgal į turinį](#)

Audros, gaisrai. Audrų metu didžiausias pavojus kyla dėl žaibavimo. Žaibai sukelia gaisrus ar pakyla elektros įtampa. Pagrindinės gaisrų priežastys: nesaugus degių medžiagų laikymas, neatsparių ugniai medžiagų naudojimas pastato konstrukciniams ir apdailos elementams, ugnies sekimo ir gesinimo įtaisų trūkumas, nepakankama aparatūros apsauga nuo ugnies.

Vandens poveikis. Vanduo į patalpas dažniausiai patenka dėl lietaus, potvynių, santechninės sistemos sutrikimų, šildymo įrangos gedimų, oro vėsinimo sistemų darbo sutrikimų, gaisrų gesinimo pasekmių. Vanduo, patekdamas į darbo patalpas, daugiausia pavojaus sukelia energijos tiekimo šaltiniams bei techninei įrangai.

Elektros instaliacijos degimas. Kai užsidega kabeliai, galimos tokios pasekmės: trūkinėja jungtys, susidaro nuodingosios dujos. Ugniai atspariomis medžiagomis nepadengti kabeliai padeda gaisrui išplisti. Jeigu kabeliai uždari, stichija nepastebėta gali išplisti po visą sistemą.

Rekomenduojamos priemonės. [Atgal į turinį](#)

Infrastruktūrinės: pastatai (patalpų išdėstymas, priešgaisrinė apsauga, oro vėsinimo ir drenažo sistemos), techninė įranga (techninės įrangos išdėstymas).

Administracinės: darbo organizavimas (darbo vietos priežiūra), netikėtumų planavimas (“Pavojaus” situacija, IS atsarginių dalių įsigijimo planavimas).

Telekomunikacinės: techninė įranga (kabeliai).

1.2. Netyčinės subjektyvios aplinkybės [Atgal į turinį](#)

1.2.1. Pasekmės [Atgal į turinį](#)

Duomenų pažeidimo poveikio laipsnis nėra labai didelis. Dažnai galimi padariniai nebūna labai pavojingi: informacija pasiūsta kitam adresatui; netikslūs duomenys; pradingo dalis informacijos; prarasta informacija po paskutinio kopijavimo; sugadinta operacinė sistema. Išimtiniais atvejais padariniai gali būti tragiški: kompiuterio virusas, gadinantis informaciją, pateko į kompiuterių tinklą, ypač, jei vietinis kompiuterių tinklas yra didelis; dar labiau, jeigu informacinės sistemos komponentai susieti vienas su kitu per išorinį tinklą; sugadinta visa informacija, nėra atsarginės kopijos.

1.2.2. Veiksniai, kylantys dėl darbo organizavimo nesklandumų [Atgal į turinį](#)

Vidaus taisyklių pažeidimai. Svarbu, kad su vidaus darbo tvarkos taisyklėmis susipažintų ir jas vykdytų kiekvienas darbuotojas.

Priežiūros trūkumas. Sistemos priežiūra turėtų būti nuolatinė. Į saugomas patalpas darbuotojai neturi patekti be leidimo.

Resursų kontrolė. Jei programinės įrangos arba organizacinės technikos naudojimo teisės suteikiamos neįgaliotam asmeniui, sumažėja duomenų slaptumas, gali sutrikti kompiuterių darbas. Bet kokio tipo resursai turi būti įgyjami ir naudojami pagal paskirtį, ir tai turi stebėti duomenų apsaugos įgaliotinis ar kitas specialiai paskirtas darbuotojas. Dėl resursų trūkumo gali nutrūkti su IS susijusios operacijos ar net visos sistemos darbas, taip pat atsitinka esant netinkamam resursų parinkimui. Kiekvienas resursas turi turėti pilną dokumentų komplektą. Už neturinčių licencijos produktų naudojimą gresia administracinės nuobaudos. Be to, nelegaliuose produktuose gali būti paslėptų klaidų.

Netinkamai paskirstytos vartotojų teisės. Vartotojų teisės apibrėžiamos taikant du principus: tam tikros funkcijos leidžiamos, kitos ribojamos arba uždraustos. Tai gali klaidingai užkirsti kelią pagrindinėms funkcijoms atlikti ir efektyvus darbas kompiuteriu taps nebeįmanomas. Keletui skirtingų vartotojų dirbant ta pačia duomenų baze, duomenų saugumui dėl prasto darbo organizavimo gali kilti grėsmė. Dažnai keičiasi nešiojamųjų kompiuterių naudotojai, todėl gali kilti pavojus dėl slaptųjų duomenų ar virusų, paliktų kietajame diske. Dėl neregistruojamo kompiuterių "judėjimo" gali dingti organizacinė technika, galimas duomenų nutekėjimas.

Programinės įrangos testai. Programinei įrangai tikrinti dažniausiai naudojami tikri duomenys. Tačiau bandymų metu gali kilti sunkumų. Kai duomenų bazės yra viešai neskelbtinos arba slaptos, testo metu saugomus duomenis gali pasiekti neturintys leidimo darbuotojai. Kai eksperimentuojama darbo aplinkoje, duomenys gali nutekėti arba tapti neprieinami. Jei nauja programinė įranga yra nepakankamai gerai patikrinta arba pateikta be instrukcijų, instaliuojant gali atsirasti nepastebimų klaidų – tai pakenktų efektyviam IS darbui. Dažnai nekreipiama dėmesio į tai, kad programinės įrangos tikrinimo išlaidos yra kur kas mažesnės už galimas išlaidas dėl padarytų klaidų.

Netinkama duomenų laikmenų priežiūra. Perdavimui naudojamos laikmenos labai svarbios duomenų saugumui ir prieinamumui. Jei jos nėra tinkamai susistemintos, užkoduotos ir perduotos įgaliotam asmeniui, gali iškilti grėsmė duomenų saugumui.

Nepakankamas linijų pajėgumas ir apsauga. Dažnai pasitaikanti planavimo klaida - tinklai kuriami esamam organizacijos pajėgumui. Kai pagausėja duomenų srautai, naujų kabelių tiesimo išlaidos kartais yra daug didesnės negu pirminių. Dėl trūkstamos tinklų kabelių dokumentacijos atsiranda nesklandumų norint patikrinti, pataisyti linijas, pakeisti kabelius ar tiesti naujas linijas. Elektros energijos paskirstymo taškai dažniausiai būna neužrakinti bei laisvai pasiekiami, o tai suteikia daugybę galimybių manipuluoti (pasinaudoti) energijos tiekimu.

Kompiuterių integravimas į tinklą. Kai kompiuteris įjungiamas į serverio palaikomą tinklą, atsiranda papildomų priėjimų prie tinklo, kurie nėra pakankamai kontroliuojami. Vartotojas gali pats nustatyti konfigūraciją, kuri leistų pasiekti kitų vartotojų duomenis. DOS terpės kompiuteris, įjungtas į Windows NT tinklą gali sukelti problemų. Kai tinklo duomenys saugomi kietajame diske ar magnetinėse laikmense, su saugumu susijusi informacija be serverio protokolo įrašų

gali būti pasiekiami pašalinių. Be to, kyla pavojus, kad į sistemą gali patekti virusų. Jei serverio palaikomam kompiuterių tinklui yra vartojama Windows terpė, asmeninė lygiateisių mazgų funkcija riboja tinklinius perdavimus. Nepakankamas sričių planavimas bei jų patikimų ryšių įvertinimas Windows NT tinkluose gali tapti klaidingų sistemos konfigūracijų priežastimi. Jeigu tinklas prie išorinių tinklų prijungiamas be papildomos apsaugos priemonių, kyla slaptų ar viešai neskelbtinų duomenų nutekėjimo grėsmė. Protokolo duomenys naudojami, nustatant įsilaužimą į IS arba kitokius bandymus pakenkti saugumui. Duomenys turėtų būti stebimi nuolat. Organizacijos plečiasi ir dažnai pradžioje projektuoto tinklo galimybės vėliau netenkina visų vartotojų. Tai varžo ir lėtina visos IS darbą.

Windows apsaugos trūkumai. Jeigu Windows NT sistemoje instaliacijos metu nėra specialiai atsižvelgiama į apribojimus, kiekvienas vartotojas gali pasiekti kiekvieną bylą bei katalogą. Be to, administratoriaus slaptažodis nėra apsaugotas nuo pakartotinių spėliojimų, dėl to didesnė įsilaužimo galimybė. Netinklinėje Windows 95 versijoje neįmanoma nuspėti asmeninių vartotojų galimų veiksmų, todėl neįmanoma nustatyti, ar konkretus asmuo pakenkė saugumui.

UNIX saugos trūkumai. UNIX terpės programos naudojamos didžiulių duomenų bazių kaupimui. Tarp saugomų duomenų galima aptikti vartotojų veiksmų aprašymų, kurie gali sudominti įsilaužėlius. Todėl svarbu skirti pakankamai dėmesio tos informacijos slaptumui išsaugoti bei užkirsti kelią jos nutekėjimui.

Novell Netware saugumo trūkumai. Novell Netware serverį laikant nesaugiose patalpose, kyla grėsmė visai IS. Serverį pasiekus tiesiogiai, galima pakenkti visam sistemos saugumui. Operacinė sistema Novell Netware 3.x turi daugybę apsaugos priemonių, tačiau jos neveikia automatiškai, o reikalauja specialaus suaktyvinimo po serverio paleidimo.

Nepakankamas fakso medžiagų tiekimas. Faksui funkcionuoti reikalingos popieriaus atsargos bei pakankamai spausdinimo resursų (pvz.: rašalo, tonerio). Jų pritrūkus, gaunami pranešimai saugomi atmintyje, tačiau labai tikėtina, kad dėl ribojamos laisvos vietos bus prarasta dalis pranešimų.

Rekomenduojamos priemonės. [Atgal į turinį](#)

Infrastruktūrinės: techninė įranga (tinklų tiesimas, tinklų priežiūra).
Administracinės: darbo organizavimas (IS priežiūra, paslaugos darbuotojams bei lankytojams, teisių suteikimas ir priežiūra, programinės įrangos apsauga, tinklo saugos strategija, lygiateisių mazgų tinklo saugos strategija, Windows NT kliento-serverio tinklo saugumo strategija, Novell Netware serverio sauga, Windows 95 sauga, faksų sistemos priežiūra), personalas (lygiateisių mazgų tinklų saugos funkcijų taisyklingas naudojimas), netikėtumų planavimas (reikalavimų tyrimas, IS atsarginių dalių įsigijimo planavimas, duomenų saugumas, Windows NT priežiūra, Windows 95 priežiūra).

Techninės ir programinės: programinė įranga (garantuota sistemos priežiūra, saugūs įsiregistravimai, programinės įrangos apsauga, vidinio tinklo apsauga, UNIX apsauga, Windows 95 ir WfW apsauga, Windows NT apsauga).

Telekomunikacinės: programinė įranga (tinklo valdymas, duomenų siuntimas, UNIX tinklas, Windows tinklai).

1.2.3. Veiksniai, susiję su techninės ir programinės įrangos gedimu [Atgal į turinį](#)

Elektros energijos tiekimo gedimas. Pagrindinės priežastys – nesklaidumai tiekimo tinkle, iš anksto nepaskelbti linijų taisymo darbai, kabelių pažeidimai. Nuo elektros energijos priklauso ne tik IS darbas, bet ir tokių šalutinių grandžių, kaip oro vėsintuvai, gaisro sekimo sistemos, vandens spaudimo reguliavimo aparatai ir kt., darbas. Kabelius, kuriems naudojama elektros signalo perdavimo sistema, veikia magnetiniai ir elektros laukai. Pažeidimus lemia trys pagrindiniai faktoriai: dažnio kitimo ribos, kabelio apsauga, apsaugos priemonės, naudojamos duomenų perdavimo metu. Kiti aplinkos veiksniai (aukšta temperatūra, stiprios mechaninės perkrovos) irgi turi įtakos. "Kryžminis ryšys" – linijos gedimas, klaidai atsiradus ne dėl aplinkos poveikio, bet dėl signalų perdavimo srovių gretimose linijose. Poveikis priklauso nuo kabelio struktūros ir nuo elektrinių perduodamos elektros energijos parametrų. Įtampos kitimai gali būti

įtakoti bet kurioje tiekimo sistemos vietoje – tiek sutrikus elektros tiekimui stotyje, tiek sudegus laidams įtaiso vidinėje grandyje. Srovės pakitimų pagrindinė priežastis – apsauginis ir neutralus laidininkas tiesiami kartu ir atskiriami tik išskirstymo taškuose. Kintama srovė gali pažeisti apsauginį sluoksnį ir tampa pavojinga personalui, prižiūrinčiam tiekimo sistemą.

Kitų IS grandžių veiklos nesklandumai. Pastato viduje yra daugybė tinklų, nuo kurių priklauso visų IS dalių veikimas. Dažni incidentai įvyksta dėl šildymo, vandens bei dujų tiekimo, ugnies gesinimo, kanalizacijos sistemų gedimo. Vienos sistemų gedimas gali paveikti kitų veiklą. Baterija dažnai naudojama kaip vidinis mobilių IS elementų energijos tiekimo šaltinis. Dėl laiku nepakrautų baterijų gali kilti nesklandumų ir duomenys gali dingti. Dėl techninių klaidų ar išorės veiksmų (pvz.: operacinės klaidos, senėjimo procesai) apsaugos priemonės tampa mažiau efektyvios ar visai netinkamos naudoti. Esant mechaninėms apsaugos priemonėms (pvz.: elektroninės durų spynos) galimi dažni gedimai, dėl kurių neįmanoma daugiau naudoti aparatūros arba netgi patalpų, išleidžiama daug lėšų bei sugaištama laiko, kartais tenka pakeisti visą apsaugos sistemą.

Prisijungimas prie IS. Tinklai suteikia daugiau galimybių pasiekti duomenis. Be to, plečiant sistemos apimtį, klaidų tikimybė didėja. Jei yra žinomas NIS srities pavadinimas, kiekvienas kompiuteris gali tapti klientu, visi NIS sąrašai (ir slaptažodžių sąrašai) tampa prieinami. Jei yra gaunamos administratoriaus teisės, bet kuriuos duomenis infiltruotu kompiuteriu–klientu galima gauti anksčiau nei pačiu serveriu. Naudojantis X–Windows terpe visi vartotojai gali paveikti X vartotoją ar X serverį. Šis serveris nesistengia nustatyti vartotojo tapatumo, todėl yra neįmanoma nustatyti, iš kurio kliento yra gaunami duomenys ar kuris pasisavina informaciją.

Programinės įrangos klaidos. Programinės įrangos pažeidžiamumas – vartotojams nežinomos programavimo klaidos, didinančios visuotinę IS gedimo grėsmę. Klaidų tikimybė didesnė, naudojant sudėtingesnę ar deramai nepatikrintą programinę įrangą.

Duomenų netekimas. Duomenų praradimas pasireiškia laikinu darbo procesų sustojimu arba net finansiniais nuostoliais ir įtaka tretiesiems asmenims. Pagrindinės priežastys – magnetinių laikmenų išsimagnetinimas dėl aplinkos poveikio bei nusidėvėjimo arba magnetinių laukų poveikio, nerūpestingas duomenų ištrynimasis, bylų, užkrėstų virusu, pašalinimas, pavienių duomenų laikmenų (kietųjų diskų, diskelių, kasečių ar juostų) skaitymo įrenginių mechaninio poveikio, kompaktinių diskų paviršiaus pažeidimų, dėl ribotos atminties įrenginių talpos, papildomų energijos šaltinių nusilpimo.

Windows 95 terpė. Problemų gali kilti, jei yra pasirinktas automatiškas kompaktinio disko nustatymas; išsaugant atsarginę bylą Windows 95 terpėje, ilgus pavadinimus reikia pakeisti trumpais. Pradiniai pavadinimai gali būti atstatyti ta pačia programa, tačiau kartais informacija gali dingti ar bylos tapti neperskaitomos dėl kompiuterio katalogų struktūros pakitimo.

Fakso pranešimo siuntimas. Klaidingai sujungus ir išsiuntus faksogramą kitam adresatui, nuteka duomenys, be to, pranešimas nepasiekia reikiamo adresato. Klaidos informaciją gali paversti nesuprantama ar visai neprieinama gavėjui. Tai ypač pavojinga, jeigu gavėjas klaidų nepastebi.

Rekomenduojamos priemonės. [Atgal į turinį](#)

Administracinės: darbo organizavimas (duomenų laikmenos, programinės įrangos apsauga, Windows 95 sauga, telefono automatinio atsakiklio aparatų priežiūra), personalas (darbuotojų supažindinimas su telekomunikacinėmis priemonėmis), netikėtumų planavimas (duomenų saugumas, Windows 95 priežiūra).

Techninės ir programinės: techninė įranga (fakso sistemos sauga), programinė įranga (saugūs išregistravimai, programinės įrangos apsauga, duomenų laikmenų priežiūra, Windows 95 ir WfW apsauga).

Telekomunikacinės: techninė įranga (serverio priežiūra, faksogramų siuntimas), programinė įranga (NFS ir NIS apsaugos mechanizmas).

1.2.4. Veiksniai, kylantys dėl darbuotojų klaidų [Atgal į turinį](#)

Netinkamas IS vartojimas. Dažniausia priežastis – nepakankamas rizikos veiksnių įvertinimas, personalo aplaidumas bei vidaus darbo tvarkos taisyklių nesilaikymas, netinkamas visos sistemos valdymas.

Įsijungimas į tinklą. Dėl papildomo įsijungimo gali sutrikti įprastas sistemos funkcionavimas (pvz.: pažeidžiama tinklo adresavimo sistema, atsiranda ryšio trūkių), pažeidimų rizika didesnė jeigu nepakankamai apsaugoti kabeliai.

Duomenų laikmenos. Persiuntimo metu duomenų laikmenos turi būti tinkamai apsaugotos, kad nedingtų, nepatektų kitam adresatui ir nebūtų pažeistos mechaniškai. Perduodamose laikmenose turi pasilikti tik perdavimui skirta informacija. Magnetinių laikmenų tapatybę UNIX terpėje gali būti nustatoma pagal duomenis, esančius */etc/exports*. Yra apsaugotos tik bylos, priklausančios pagrindiniam katalogui.

Klaidos transportuojant informaciją. Konfigūravimo arba programinės elektroninio pašto siuntimo įrangos klaidos, naudojimas faksu gautais dokumentais, kurie neturi juridinės galios, automatinio atsakiklio operatoriaus klaidos, PBX gedimai dėl personalo kvalifikacijos stokos sukelia daugybę informacijos saugumo problemų.

Duomenų pažeidimas dėl vartotojo klaidos. Dėl aplaidumo ar neišsamaus instruktažo sugadinama aparatūra, pažeidžiami duomenys, prarandama duomenų kontrolė. Taip gali atsitikti pasirenkant bei naudojant netinkamą programinę įrangą.

Teisių suteikimas. Teisės į viešai neskelbtinus ir slaptus duomenis bei IS programinę įrangą turi būti teikiamos tik darbuotojams, kuriems tai reikalinga atliekant jų pagrindines užduotis. Jei teisių nesuteikiama pakankamai ar jų turima per daug, tai kenkia darbo našumui ir sistemos saugumui. Naudojant Windows NT terpę, reikalinga slaptažodžių sistema, kad kiekvienas vartotojas turėtų apibrėžtas teises, čia galima nustatyti teisių apribojimus tiek kiekvienam kompiuteriui, tiek vartotojui. Esant Windows NT tiktai sistemos administratorius gali suteikti tokias teises. Atlikti pagrindines funkcijas leidžiama visiems vartotojams, tačiau ir tai gali sukelti nesklandumų. Taip pat verta prisiminti, kad naudojant šias terpes, teises naudotis katalogu reikia pakeisti, įsiregistruojant naujam vartotojui. WfW aprėpia pašto bei laiko planavimo programą *Schedule+*. Jeigu bendra pašto dėžute naudojasi keletas vartotojų, laiko planavimas jiems irgi gali būti prieinamas. Standartinėje versijoje asmeniniai kalendoriaus įrašai yra matomi kitiems vartotojams, net be jų savininko žinios ir leidimo. Problemų gali kilti ir kai vienu kompiuteriu dirba keletas vartotojų, dėl apsileidimo ar patogumui vartotojai ne iki galo išsiregistruoja ar išsiregistruoja.

Operacijos su slaptažodžiais. Windows 95 ir WfW terpėse reikalingi slaptažodžiai saugomi bylose *[vartotojo vardas].pwl*, tačiau naudojantis Internetu įmanoma gauti programų, iššifruojančių *.pwl bylas nežinant slaptažodžio. Todėl turi būti sukurta ir atitinkama bylų duomenų apsauga.

Rekomenduojamos priemonės. [Atgal į turinį](#)

Infrastruktūrinės: techninė įranga (tinklų tiesimas).

Administracinės: darbo organizavimas (IS priežiūra, IS administratorius, teisių suteikimas ir priežiūra, slaptažodžių bei raktų vartojimas, duomenų laikmenos, tinklo saugos strategija, lygiateisių mazgų tinklo saugos strategija, Windows 95 sauga, faksų sistemos priežiūra, telefono automatinio atsakiklio aparatų priežiūra, PBX priežiūra), personalas (bendras instruktažas, darbo aplinkos gerinimas, IS administratorius, darbuotojų supažindinimas su telekomunikacinėmis priemonėmis, lygiateisių mazgų tinklų saugos funkcijų taisyklingas naudojimas), netikėtumų planavimas (Windows 95 priežiūra, PBX sauga).

Techninės ir programinės: techninė įranga (PBX techninė apsauga, fakso sistemos sauga), programinė įranga (slaptažodžiai, duomenų laikmenų priežiūra, UNIX apsauga, Windows 95 ir WfW apsauga).

Telekomunikacinės: techninė įranga (faksogramų siuntimas), programinė įranga (tinklo valdymas, duomenų siuntimas, kodavimas, UNIX tinklas, Windows tinklai).

1.3. Tyčinės subjektyvios aplinkybės [Atgal į turinį](#)

1.3.1. Pasekmės [Atgal į turinį](#)

Duomenų pažeidimo poveikio laipsnis – labai didelis, padariniai rimti: duomenys nepilni ir netikslūs ar pilnai sugadinti; duomenų bazių įrašai suklastoti ir nekorektiški, sunku atrasti klaidas bei suklastotą informaciją; dėl vagystės prarasti ne tik duomenys iš duomenų bazių, bet ir visos atsarginės kopijos; neveikia kompiuterinės programos ir operacinė sistema; visa kompiuterinė sistema neveikia.

1.3.2. Veiksniai, kylantys dėl tyčinių subjektyvių aplinkybių [Atgal į turinį](#)

Neteisėtas naudojimas IS. Naudojimas gali būti įvairus: klaidingų duomenų įvedimas, teisiu ar operacinės sistemos programinės įrangos pakeitimai ir t.t. Vartotojas gali viršyti vartotojo teises, bandyti atspėti kitų vartotojų slaptažodžius. Dažnai apsaugos priemonėmis piktnaudžiaujama dėl patogumo – pvz.: neišlaptinama kodinės spynos teisinga kombinacija, trumpam pasitraukus iš darbo vietos, įrenginiai nėra saugomi, todėl įmanoma naudotis aparatūra nežinant apsauginių kodų.

Fizinis įsibrovimas į IS. IS gali būti pažeista tiek pačioje organizacijoje, tiek iš išorės. Be tiesioginių materialių nuostolių grėsmė kyla ir IS saugumui – galima vagystė ir neteisėtas naudojimas. Naudojant mobilias IS priemones dėl transportavimo kyla didesnė vagystės grėsmė negu naudojantis stacionariomis. Antpuolio tikimybė didesnė, jeigu vyksta politiniai neramumai, organizacija įsikūrusi netoli demonstracijų vietos. Vandalizmo aktas gali būti įvykdytas tiek įmonės darbuotojų (personalo problemos, prastas organizacijos mikroklimatas), tiek pašalinių.

Įsiterpimas į tinklus. Įsiterpimas į linijas yra paprastas, tačiau sunkiai aptinkamas pažeidimas. Be įsiterpimo į linijas, naudojimuisi jomis priskiriami: sukurti nesankcionuoti ryšiai organizacijos viduje ir už jos ribų, linijų naudojimas asmeniniais tikslais. Pažeidėjas pasinaudoja duomenimis, juos pasisavindamas ar pažeisdamas. Yra du pagrindiniai jungties būdai – naudojant modemą per valdymo taškus bei tiesioginis per DISA. Įsilaužėliams atspėjus slaptažodžius, gali būti visiškai pažeista sistema, galima netekti duomenų, patirti finansinių nuostolių. Per modemą galima patekti į IS, prisiskambinant iš išorės ir liekant nepastebėtam. Grėsmė kyla, jei teisėtas vartotojas neišsiregistruoja iš sistemos, ir jam baigus darbą, ryšio linija lieka atvira. Jeigu informacija yra siunčiama tinklu nekoduota, ji gali būti lengvai perskaitoma, naudojant tinklo analizės priemones. UUCP (UNIX–UNIX) programinio paketo pagalba IS gali keistis skirtingų standartų bylomis, be to, galimas distancinis komandų vykdymas. Grėsmė darbo efektyvumui ir duomenų saugumui kyla, kai teisių suteikiama nepakankamai ar per daug. Jeigu tinklas be papildomų apribojimų, vartotojai gali paprastai naudotis kituose kompiuteriuose įmontuotais mikrofonais, taip sekdami patalpas.

Vartotojo teisių pažeidimas. Vartotojo (arba administratoriaus) teisių pažeidimu laikomas asmens teisėtas arba nelegalus (slaptas) naudojimas kito asmens (arba savo) teisėmis, siekiant pakenkti sistemai ar jos vartotojams. Yra daugybė galimybių išnaudoti sistemos administratoriaus teises – pradedant nesankcionuotu bylų skaitymu, vartotojų įsiregistravimo duomenų pakeitimu, baigiant bandymu paveikti protokolą, vartotojų veiksmų sekimu, visos sistemos išjungimu ir t.t. Priklausomai nuo terpės, kurioje veikia IS, įsilaužėliai gali naudotis svetimomis teisėmis, t.y. naudotis kito asmens atpažinimo duomenimis; keisti kompiuterio bei įsiregistravimo vardus; atspėjus slaptažodį, pasiekti norimą riboto skaitymo katalogą; ištrinti slaptažodžio bylą [*vardas*].*pwl*, tuomet įmanoma įsiregistruoti ir nežinant vartotojo slaptažodžio. Paslaugų ribojimas užkerta kelią standartinių įrenginių naudojimui, o pritrūkus specialiujų ribojimų vartotojas gali neatsargiai pasinaudoti savo teisėmis.

Duomenų atskleidimas. Slaptieji duomenys gali būti atskleisti pasinaudojant organizacijos darbuotojais, taip pat darbuotojai gali neleistinai pakeisti privilegijas, šitaip sutrikdydami sistemos darbą ar duomenų rašymo/skaitymo ribojimus. Duomenų laikmenų transportavimo metu neįgaliotas asmuo gali lengvai atlikti duomenų kopijavimą. Atliekamos sistemos modifikacijos gali sukelti nesklandumų, nes apie jas ne visuomet pranešama.

Pranešimų tēkmēs analizē. Tēkmēs analizē suteikia žinių apie vartotojo veiksmus. Panašiai yra bandoma gauti elektroninio pašto bei įprastus adresus, kad būtų galima išsiųsti nepageidaujamą informaciją.

Siuntimo aprašymo protokolai. IP paketas leidžia nustatyti saugų persiuntimo būdą. Tačiau šis aprašymas siuntimo metu gali būti pakeičiamas, nukreipiant į neapsaugotą transportavimo būdą. IP "triukas" – įsijungti į sistemą, pateikiant tariamus IP numerius ir taip ją suklaudinant. Vietiniame tinkle vartojant ARP, galimi dar veiksmingesni "triukai". Per ARP sužinojus įrenginio adresą, šiuo aparatu galima kontroliuoti visą tinklą. ICMP persiunčia užduočių, klaidų bei diagnostinę informaciją. Veiklos pažeidimai galimi dėl siuntimo kelio pakeitimo arba prisijungimo nutraukimo ir tinklo pažeidimo. RIP arba OSPF protokolai yra skirti siuntimo kelių iš vienos sistemos į kitą pakeitimų nustatymui. Visi procesai vyksta be papildomų patikrinimų, todėl galimos klaidos.

Naudojimasis telekomunikacinėmis priemonėmis. Informacijos nutekėjimo priežastys: konferencinė funkcija (galimybė kalbėtis daugiau dviejų asmenų); neteisingas pokalbių paskirstymas; galimybė prisiskambinti organizacijos telefonu skirstytuvu ir jo pagalba susisiekti su pageidaujamais asmenimis; galimybė, kad darbuotojai, pasinaudoję kolegų aparatais, skambins savais tikslais; yra galimybė perskaityti paskutinius skambinusiųjų numerius, pasiklausti svetimų pokalbių (tiesiogiai taip pat pasinaudojant pasiklausymo aparatais arba naudojant PBX terminalų tolimosios krypties prisiskambinimo galimybes). PBX instaliacijų metu viešai neskelbtini arba slapti duomenys saugomi kietuose diskuose. Atnaujinant įrangą, šie diskai atiduodami PBX gamintojams – duomenys gali nutekėti.

Naudojimasis fakso aparatu. Informacijos nutekėjimo priežastys: fakso aparatas yra prieinamas visiems organizacijos darbuotojams; naudojant terminio spausdinimo aparatą yra galimybė vidinės plėvelės pagalba atkurti net keletą šimtų paskutinių pranešimų; pasinaudojant svetimu vardu, galima suklaidinti fakso pranešimo gavėją; dažnai renkamo numerio užprogramavimo funkcija (galimybė perprogramuoti atmintyje išsaugotą numerį); faksas taip apkraunamas, kad tampa nefunkcionalus.

Telefonas automatinis atsakiklis. Automatinio atsakiklio atmintį užpildžius tuščiais pranešimais ribojama galimybė išsaugoti naujus pranešimus arba išsaugomi naujieji pranešimai, panaikinus gautus anksčiau. Naudojantis telefonu automatinio atsakikliu bei žinant apsaugos kodus, yra galimos tokios nuotolinio veikimo funkcijos: kambario sekimas, išsaugotų, gaunamų bei išsiunčiamų pranešimų valdymas, skambučių nukreipimo numerių keitimas, įrašų juostos atsukimas ar persukimas, kitos elektroninės įrangos veikimo įtakojimas, automatinio atsakiklio išjungimas.

Kompiuteriniai virusai. Kompiuterinis virusas yra vartotojo nevaldoma programa, skirta duomenų naikinimui ar pažeidimui. Jie gali būti sukelti tyčia arba atsitiktinai. Dažniausiai pasitaikantys virusai yra skirti DOS ir Windows terpėms. UNIX terpei skirtų virusų yra žymiai mažiau. Grėsmė duomenis užkrėsti makro virusais kyla keičiantis bylomis (tiek vartojant elektroninį pašta, tiek magnetines laikmenas). Jie pradeda veikti ir patys, ir dėl vartotojo įtakos. "Trojos arkliai" turi antrinį, slaptą poveikį – skaudžių rezultatų dažnai sulaukiama dėl vėlesnio pasinaudojimo gauta informacija. Visos vartotojų programos gali būti naudojamos kaip nešėjos.

Novell Netware pažeidimas. Novell Netware sistema gali būti pažeista dviem būdais. Pirmasis siejamas su bandymu atspėti vartotojo slaptažodį. Paprastas vartotojas, atspėjęs sistemos administratoriaus slaptažodį, gali jį pakeisti arba sau priskirti tokias pačias teises. Įmanoma naudotis visa informacija, kol ji nėra papildomai apsaugota (pvz.: užkoduota). Sėkmingai įsiregistravus į Novell Netware serverį, vartotojams sukuriama asmeninė tinklo aplinka. Naudojant schemas komandas įmanoma naršyti po Novell Netware serverį. Jeigu privilegijos nėra tinkamai paskirstytos, vartotojas gali pasiekti informaciją, kuri paprastai nėra skiriama jam. Naujiems vartotojams registruojantis pirmą kartą iš jų nereikalaujama slaptažodžių. Kai vartotojas turi daugybę teisių, gali būti "pagrobtas" jo laisvas vardas. Taip pat skirtingose Netware Utilities versijose (pvz.: 3.75, 3.76) administratoriui panaudojus naująjį slaptažodį,

sistema jį tinklu siunčia nekoduotą. Antras pažeidimo būdas - darbas baigiamas netinkamai arba *ABEND* įvyksta, kai Netware operacinė sistema nebet kontroliuoja tinklo. *ABEND* galima sukelti ir tyčiniu būdu.

Rekomenduojamos priemonės. [Atgal į turinį](#)

Infrastruktūrinės: techninė įranga (tinklų priežiūra, nešiojamųjų kompiuterių saugumas).
Administracinės: darbo organizavimas (teisių suteikimas ir priežiūra, slaptažodžių bei raktų vartojimas, saugumo informacija, duomenų laikmenos, tinklo saugos strategija, lygiateisių mazgų tinklo saugos strategija, Windows NT kliento-serverio tinklo saugumo strategija, Novell Netware serverio sauga, Windows 95 sauga, faksų sistemos priežiūra, telefono automatinio atsakiklio aparatų priežiūra, PBX priežiūra, modemų priežiūra), personalas (IS administratorius), netikėtumų planavimas (kompiuteriniai virusai, duomenų saugumas, Windows NT priežiūra, Windows 95 priežiūra, PBX sauga, CMOS RAM apsauga).
Techninės ir programinės: techninė įranga (nešiojamųjų kompiuterių apsauga, apsauga nuo patalpų pasiklausymo, PBX techninė apsauga, fakso sistemos sauga), programinė įranga (duomenų laikmenų priežiūra, vidinio tinklo apsauga, UNIX apsauga, Windows 95 ir WfW apsauga, Windows NT apsauga).
Telekomunikacinės: techninė įranga (serverio priežiūra, faksogramų siuntimas, modemas), programinė įranga (tinklo valdymas, nuotolinio ryšio apsauga, NFS ir NIS apsaugos mechanizmas, duomenų siuntimas, kodavimas, saugumas, naudojant Internetą, UNIX tinklas, Windows tinklai).

2. Duomenų apsaugos priemonių aprašymas [Atgal į turinį](#)

2.1. Infrastruktūrinės priemonės [Atgal į turinį](#)

2.1.1. Pastatai [Atgal į turinį](#)

Patalpų išdėstymas. Renkantis ar įvertinant esamą pastato vietą, reikia atsižvelgti į šalia esančių transporto trasų sukeltų vibracijų, autoįvykių poveikį, galimybę išsilauželiams pasprukti nepastebėtiems, arti esančius radijo siųstuvus, vandens telkinius, elektrines ar specialiąsias gamyklas. Statant pastatus, įrengiant bei keičiant IS turi būti atsižvelgiama į oficialius standartus, sukurtus daugeliui technologijos sričių. Pagrindinė priežastis – garantuoti vartotojų saugumą darbo metu. Patalpos, turinčios didesnę rizikos potencialą, negali būti skirtos specialios paskirties patalpų įrengimui. Paskirstymo centrai turi būti įrengti atskirose patalpose. Paskirstymo linijos turi būti ir pakankamai saugios, ir lengvai pasiekiamos sugedus. Specialiosios paskirties patalpos neturi būti pažymėtos lentelėmis, atskleidžiančiomis jų paskirtį, patartina turėti šarvines duris, įėjimas į patalpas turi būti kontroliuojamas. Darbuotojams išeinant iš patalpų, privalu uždaryti langus bei duris. Reikalingos patalpų, paliekamų trumpam laikui be personalo, priežiūros taisyklės. Efektyvu įrengti išilaužimo ir gaisro nustatymo prietaisus, kurie būtų jungiami tiesiogiai į išorinių apsaugos institucijų tinklą. Minimalų saugumą gali garantuoti vietiniai davikliai, kurie pavojaus metu įjungtų vietinę signalizaciją. Vengti itin degių medžiagų sankaupos vienoje vietoje. Atsižvelgiant į horizontalių pastato perdangų keliamąją gebą, pasirinkti apsauginių sekcijų dydį. Esama bendrų apsaugos normų: langai ir durys turi būti apsaugoti nuleidžiamomis žaliuzėmis arba grotomis, rakinami nenaudojami šoniniai įėjimai, atsarginiai išėjimai apsaugoti, kad pro juos nepatektų pašaliniai asmenys, liftai nedarbo metu išjungiami. Darbuotojai turi būti informuojami apie saugos priemones bei supažindinti su vidaus darbo tvarkos taisyklėmis.

Priešgaisrinė apsauga. Būtina griežtai laikytis priešgaisrinės apsaugos tarnybos nustatytų normų. Mažus ugnies židinius geriausia gesinti rankiniais gesintuvais. Gesintuvai turi būti parinkti atsižvelgiant į saugomą aplinką, pastatyti (pakabinti) šalia saugotinių patalpų, turi būti nuolat tikrinamas jų veiksmingumas. Ypatingą dėmesį reikia atkreipti į apsauginių perskyrų kokybę, specialiai apsaugoti kabelius. Personalas informuojamas apie priemones, kurių reikia imtis, kilus gaisrui.

Oro vėsinimo ir drenažo sistemos. Patalpose, kuriose sutelkta daug veikiančių kompiuterių, reikalinga oro vėsinimo sistema, pageidautina reguliuoti ir oro drėgnumą. Oro vėsinimo

įrenginiai turi būti nuolat tikrinami. Pastato vietose, kur gali kauptis vanduo, turėtų būti įrengtas automatinis vandens aptikimas bei drenažas (pasyvus arba pneumatinis). Priklausomai nuo drenažo sistemos rūšies, reikia laikytis nustatytų priežiūros taisyklių. Patalpose, kuriose koncentruojama informacinė įranga, reikia vengti tekančio vandens vamzdynų, palikti tik pačius būtiniausius. Kaip papildomą apsaugos priemonę galima įrengti automatinį drenažą.

2.1.2. Techninė įranga [Atgal į turinį](#)

Techninės įrangos išdėstymas. Pagrindiniai kriterijai, planuojant IS išdėstymą, yra tokie: ilgo sistemos darbo bei vartotojų ergonomiškumo garantija. Keletas bendrų patarimų: elektroniniai aparatai neturėtų būti statomi šalia šildytuvų, prieš tiesioginius saulės spindulius; taip pat nestatomi šalia langų ar durų, nes juos gali pastebėti pašaliniai; turėtų būti vengiama tiesiogiai krentančios į kompiuterių ekranus šviesos, kad būtų patogiau darbuotojams. Pagrindinė taisyklė – duomenis saugančius bei svarbius veiklai įrenginius (t.y. serverio administravimo įrangą, spausdintuvus, fakso aparatus, PBX, išorinius modemus) laikyti riboto priėjimo arba stebimose patalpose. Nuošaliose vietose paliktiems įrenginiams naudoti nuotolinį naudojimo ir gedimų stebėjimą. Teisė fiziškai pasiekti modemą suteikiama tik prižiūrinčiam personalui. Duomenų laikmenos turi būti saugomos ne tik transportavimo metu, bet ir iškart po duomenų patalpinimo. IS sukoncentravus vienoje patalpoje, elektromagnetinių laukų poveikiui sumažinti galima naudoti apsauginius filtrus.

Tinklų tiesimas. Renkantis kabelius derėtų atsižvelgti į šiuos kriterijus: tiesimo vietą (pastato vidus ar išorė), aplinkos sąlygas, galimą mechaninį poveikį, specialią dangą, apsaugančią nuo ugnies ar nuo stiprių elektrinių laukų, numatyti galimų jungčių į elektros tinklą vietas. Tiesiant tinklus reikia atsižvelgti į galimą poreikių augimą ateityje. Todėl arba iš karto tiesiamas kabelis turi turėti papildomo pajėgumo, arba ateityje šalia jo gali būti nutiestas antrasis, iš anksto tam palikus vietas. Dokumentuose turėtų būti pažymėtas tikslus linijų išdėstymas, techniniai duomenys, pastabos, vartotojai įsijungę į sistemą, pavojaus zonos, naudojamos apsaugos priemonės. Dokumentai turi būti laikomi saugomose patalpose, griežtai ribojant galimų vartotojų skaičių.

Tinklų priežiūra. Elektros energijos bei telekomunikacijų vidiniai tinklai yra jungiami tiesiogiai prie išorinių linijų. Saugumo sumetimais patikimiausia įrengti izoliuotą vidinį tinklą ir jį jungti prie išorinio tik pririnkus (pvz.: siunčiant duomenis). Apsauga nuo žaibo sukeltų perkrovų gali būti išoriška ir vidinė. Perkrovų laipsnis priklauso nuo kilmės šaltinio, tačiau bet kokie įtampos svyravimai kenkia IS. IS apsaugą nuo perkrovų reikia pradėti nuo elektros energijos perdavimo linijų, toliau vidiniame energijos skirstytuve, galiausiai visuose pastato energijos šaltinių lizduose. Jeigu apsaugos priemonių neįmanoma išdėstyti visame pastate, prioritetas turi būti teikiamas svarbiausioms IS grandims (pvz.: serveriui). Nuo srovės prasiveržimų padeda apsisaugoti tinkama duomenų linijų danga. Elektros tiekimo išjungimo įtaisas rengiamas patalpose, kur gali kilti gaisras dėl įrangos perkrovų. Tiekimo išjungimo rankena turi būti įrengta šalia saugomų kambarių ir aiškiai pažymėta, tačiau šiuo įtaisu įmanoma pasinaudoti ir negresiant pavojui. UPS dėka trumpi elektros energijos tiekimo nutraukimai nekelia pavojaus. UPS leidžia sėkmingai baigti darbą ir prasidėjus ilgiems tiekimo nesklandumams, tačiau nutūkus pagrindiniam energijos tiekimui, reikia numatyti ir automatinį UPS atsijungimą.

Nešiojamųjų kompiuterių saugumas. Saugaus transportavimo taisyklės: kuo trumpiau kompiuterį palikti be priežiūros; patalpos turi būti rakinamos paliekant net trumpam laikui; paliekant automobilyje patartina paslėpti; naujaisi nešiojamieji kompiuteriai turėtų būti prirakinami. Nuolat turi būti tikrinama, ar jų baterijos tinkamos darbui. Papildomai turi būti įdiegta dokumentų vartotojams sistema - naudojimosi instrukcijos ir grafikai, apsaugos priemonių taikymas.

2.2. Administracinės priemonės [Atgal į turinį](#)

2.2.1. Darbo organizavimas [Atgal į turinį](#)

IS priežiūra. Turėtų būti raštiškai įgalioti ir visam personalui žinomi asmenys (duomenų apsaugos įgaliotiniai), atsakingi už šias funkcijas: duomenų saugojimas, archyvų priežiūra,

laikmenų transportavimas, duomenų perdavimas, laikmenų sunaikinimas, IS dokumentai, slaptažodžių vartojimas, teisių skirstymas, resursų kontrolė, įrenginių ir programinės įrangos įsigijimas bei priežiūra, taisymo darbai, duomenų slaptumas, apsauga nuo virusų, auditas, pirmosios pagalbos priemonės. IS saugos priemonės tvirtinant dokumentu, patartina naudoti pagalbinį sąrašą, aprėpiančiu vartotojo vardą, instaliavimo sritį, konfigūracijos aprašymą, teisių suteikimo priemonės, naudojamus įrenginius bei programinę įrangą, duomenų atsarginio saugojimo laiką, atliktus taisymo darbus, virusų patikrinimus, slaptažodžių pakeitimo laiką, kontaktą pavojaus atveju. Svarbu sukurti IS vartotojų instrukcijas. Į instrukcijas įtraukiama – fizinė bei loginė tinklo struktūra (jeigu sistema tinklinė), vartotojų profiliai, duomenų kopijų saugojimo apibūdinimas. Keičiantis IS, svarbu atnaujinti konfigūracijos aprašymą.

IS administratorius. Administratorius yra atsakingas už sistemos kasdienį darbą bei saugos garantavimą. Rekomenduojama jį paskirti ir duomenų apsaugos įgaliotiniu. Jo slaptažodį patartina išskaidyti į dvi dalis ir skirti dviem darbuotojams, kurie nėra daliniai administratoriai. Patartina paskirti papildomų administratorių, atsakingų už skirtingas funkcijas ir galinčių pakeisti sistemos administratorių. Administratorius turi nuolat tikrinti sistemą, vykdyti reikiamus pakeitimus, todėl reikia nuolat tvarkyti IS pakeitimų dokumentus.

Darbo vietos priežiūra. Darbo vieta turi būti tvarkinga. Priešgaisrinės saugos taisyklės turi atitikti Priešgaisrinės tarnybos keliamus reikalavimus. Sistemingai reikia atlikinėti saugos priemonių patikrinimus. Patartina patalpose su IS technika uždrausti rūkyti.

Paslaugos darbuotojams bei lankytojams. Vartotojų veiksmų sekimas, supažindinimas su IS pakitimais, standartinių gedimų analizė, naudojimosi kompiuteriu instrukcijų sukūrimas, registruojamas IS priemonių išdavimas ir susigražinimas/perleidimas besikeičiant vartotojui - lemia gerą saugos priemonių poveikį. Be to pašaliniai lankytojai turi būti lydimi organizacijos darbuotojų, kontroliuojami įėjimai į sustiprinto saugumo reikalaujančias patalpas.

Teisių suteikimas ir priežiūra. Pastatą patartina padalinti į sekcijas, kurioms suteikiamos skirtingos teisės. Taip pat reikia apibrėžti teises, suteiktinas konkrečiam darbuotojui. Naudojimosi teisėmis patikrinimą privalo atlikti arba įėjimą kontroliuojantis darbuotojas, arba techninis įtaisas. Tinklo administravimo arba sisteminės teisės skirstomos remiantis principais: griežtas teisių ribojimas, teises turi suteikinti IS administratorius, visi paskirstymai turi būti įteisinti dokumentais, apibrėžtos kiekvieno vartotojo funkcijos ir slaptažodis, kurti vienodas funkcijas atliekančių darbuotojų grupes, reguliariai tikrinti vartotojų veiksmų ataskaitas ir įsiregistravimo bylas, vykdyti atsitiktinius patikrinimus, patartina įdiegti identifikavimo sistemą, kontroliuojančią vartotojų įsiregistravimą.

Slaptažodžių bei raktų vartojimas. Patartina įdiegti slaptažodžių kūrimo taisykles: jie negali sietis su vardais ar gimimo datomis, ilgis – bent 6 simboliai, gamintojo slaptažodžiai pakeičiami individualiais, slaptažodžiai negali būti užprogramuoti specialiais klavišais, slaptažodį turėtų žinoti tiksliai vartotojas, užrašytas slaptažodis laikytinas tiksliai užklijuotuose vokuose ir naudotinas tiksliai incidento metu, slaptažodį reikia reguliariai keisti. Saugumą sustiprinti galima tokiais būdais: nesirinkti pernelyg paprastų slaptažodžių, pakeisti individualų slaptažodį gali kiekvienas vartotojas, įsiregistruojant naujiems vartotojams – jiems suteikiamas vienkartinis slaptažodis, atlikus tris nesėkmingus bandymus – įsiregistravimas turi būti blokuojamas, slaptažodžius siųsti tinklu tiksliai užkoduotus. Organizacijoje reikia nustatyti durų rakinimo sekcijas. Patartina laikytis šių nuorodų: kabinetus grupuoti į atskiras, vienodo saugumo reikalaujančias sekcijas; atsarginius raktus laikyti saugiai; dokumentu patvirtinti raktų išdavimą, darbuotoją supažindinti su priemonėmis, kurių reikėtų imtis raktą praradus. Keičiantis darbuotojų pareigoms, būtinas raktų reikalingumo patikrinimas. Atleidžiant darbuotojus, raktai konfiskuojami. Ypatingai saugomų patalpų raktus ir spynas patartina reguliariai keisti, siekiant išvengti klautočių. Naudojant kodavimą siunčiamai slaptai informacijai apsaugoti, reikia atkreipti dėmesį į kodo sukūrimą, saugojimą, persiuntimą, pakeitimą. Nuotolinis duomenų įvedimas į serverį gali būti susektas naudojant specialius programinius paketus. Todėl kyla grėsmė, kad siunčiami slaptažodžiai pateks neįgaliotiems asmenims. Patartina atsisakyti nuotolinio valdymo.

Saugumo informacija. Patartina nuolat sekti specializuotus informacijos šaltinius, siekiant kuo anksčiau sužinoti apie skelbiamus operacinių sistemų ar programinės įrangos trūkumus. Rekomenduojama paskirti darbuotoją, kuris atsakytų už informacijos apie naujus pažeidimų būdus rinkimą bei platinimą.

Duomenų laikmenos. Duomenų apsauga yra viena svarbiausių saugos sistemų funkcijų. Duomenų laikmenos – sudėtinė IS būtinųjų resursų dalis. Tai resursai, kuriuos reikia inventorizuoti, registruoti, saugiai laikyti bei siųsti, pašalinti nereikalingus duomenis. Reikia numatyti priemones, kad jų nepasiektų pašaliniai asmenys.

Programinės įrangos apsauga. Techninių priemonių pagalba turi būti ribojamos vartotojų galimybės platinti nelegalias programas. Norint įsigyti naują programinę įrangą, rekomenduojama atlikti rinkos tyrimus, prieš tai suformulavus savo poreikius. Reikia tikrinti IS tiekėjų registravimo pažymėjimus ir siūlomos įrangos sertifikatus. Kad produktai būtų visiškai saugūs, galima leisti produktus patikrinti nepriklausomai agentūrai. Išsirinkus įrangą, turi būti atliktas jos testavimas. Testavimą patartina padalinti į tris etapus: pradinį (pvz.: virusus), funkcinį, apsaugos patikrinimus. Atlikus programinės įrangos testavimą, nustatoma pageidaujama konfigūracija, kuri nulemia darbo patogumą, mažą klaidų skaičių, saugumą. Prieš pradėdant naudoti naują programinę įrangą, ji turi būti raštiškai patvirtinama kaip tinkama darbui. Programinė įranga instaliuojama nekeičiamoje aplinkoje. Prieš tai patartina padaryti atsargines originalių duomenų kopijas. Senos programinės įrangos išinstaliavimo metu reikia pašalinti visas bylas, susijusias su ištrinama programine įranga.

Tinklo saugos strategija. Kartais turi būti atliekamas išoriškas linijų bei išskirstymo jungčių būklės patikrinimas. Ryšio išskirstytojų dokumentacija, nurodanti jų paskirtį, turi būti laikoma saugiai. Patartina paminėti tik tai naudojamas ir nebenaudojamas jungtis, neįvardijant specifinių funkcijų. Visa papildoma informacija turi būti pateikiama papildomuose dokumentuose. Yra dvi galimybės prisijungti prie Interneto – prijungti tiksliai atskirą kompiuterį ar jungti vietinį tinklą ir diegti “ugnies sieną” (Firewall). Pagrindinė strategijos taisyklė – kuo labiau apriboti išorinio nuotolinio vartotojo teises. “Ugnies sienos” konfigūracijos: filtrų naudojimas (informacija filtruojama ir kompiuteris pagal taisykles arba atmeta, arba priima gaunamus duomenis), dvipusiai vartai (programinė įranga – vienintelis dviejų (saugojamo ir nesaugaus) tinklų tarpininkas), stebimas potinklis (įkuriamas tinklas su “ugnies sienos” komponentais tarp vidinio ir išorinio tinklų). “Ugnies sienos” veikla turi būti nuolat tikrinama, kad būtų nustatytos galimos silpnosios pusės.

Lygiateisių mazgų tinklo saugos strategija. Strategija turi būti plėtojama palaipsniui: lygiateisių mazgų tinklo struktūros nustatymas, paskirstyta atsakomybė, teisių suteikimo apribojimai, standartinių vartotojų vardų sukūrimas, teisių į katalogus ir spausdintuvus suteikimas, slaptažodžių valdymas, vartotojų pareigos, mokymai. Vartotojai patys turi atlikti atitinkamus veiksmus: nustatytu laiku privalo tikrinti aktyvias jungtis, protokolų duomenis, IS administratoriaus paskirtus resursus. Šio tipo tinkle neįmanoma patikrinti teisių paskirstymo.

Windows NT kliento-serverio tinklo saugos strategija. Reikia vengti lygiateisių mazgų funkcijos Windows NT tinkluose. Tinklo struktūros nustatymas, atsakomybės paskirstymas, vardų skyrimas, vartotojų išregistravimo taisyklės, teisės, projektams skirtų katalogų sudarymas, vartotojų ir administratoriaus atsakomybė kliento-serverio tinkle, mokymai - pagrindinės saugos strategijos taisyklės. Windows NT serverio funkcijos turi būti nustatomos prieš instaliuojant operacinę sistemą. Pagal sistemos išdėstymo suplanavimą galimos sritys (grupė serverių turi panašias saugos priemones ir vartotojų duomenų bazes) ir darbo grupės (sutelkiami kompiuteriai, nesujungti į sritys). Sričių modifikacijos: pavienės, keletas pavienių, pagrindinė ir keletas pagrindinių sričių. Sukuriant saugų ryšį, galimos patikimos skirtingų sričių jungtys.

Novell Netware serverio sauga. Novell Netware 3.x serveris automatiškai neįjungia apsaugos priemonių, jas reikia suaktyvinti atskirai. Su saugumo palaikymu siejamos šios priemonės: išregistravimo ribojimai, serverio darbo laikas, *autoexec.ncf* bylos redagavimas, serverio valdymo bylos pakeitimai, išregistravimo blokavimai aptikus neleistinus bandymus, sisteminiai

įsiregistravimo standartai, serverio klaidingų registracijų bylos peržiūra, darbo grupės administratorius, darbo vietos ribojimas, standartizuota vartotojų skaičiaus konfigūracija. Saugumui palaikyti reikia imtis įvairių veiksmų, tokių kaip teisių patvirtinimas byloms ir katalogams, Netware atributų suteikimas (reguliuoja pasiekimą nepriklausomai nuo suteiktų teisių), svarbių sisteminių atsarginių bylų kopijavimas, valdymo užduočių paskirstymas plačiuose tinkluose, NCP paketo parašo naudojimas, kietojo disko naudojimo ribojimai, nereikalingos programinės įrangos blokavimas, gamintojo sukurti Novell Netware patobulinimai, virusų paieška.

Windows 95 sauga. Sukurta individuali darbinė aplinka turi būti saugoma įsiregistravimo slaptažodžio. Sistemos nurodymų projektavimas vartotojų veiksmams riboti: sisteminių nuorodų bylos sukūrimas, nuorodų standartiniam vartotojui ir kompiuteriui apibrėžimas, nuorodos administratoriui, vieno vartotojo atvejis, visų nuorodų suaktyvinimas.

Faksų sistemos priežiūra. Naudojant fakso aparatą, rekomenduojamos šios saugos priemonės: persiuntimo ataskaita, įrašų žurnalo tvarkymas. Papildomos priemonės: privalomas įsiregistravimas, vartotojų grupės konfigūracija, nenaudojamų jungčių blokavimas, atmintį apsaugoti slaptažodžiu. Kiekvienam fakso aparatui rekomenduojama paskirti atsakingą darbuotoją priežiūrai, kuris būtų atsakingas už gaunamų pranešimų paskirstymą, sudėtinių dalių tiekimo bei pašalinimo koordinavimą, fakso atminties išvalymą, taisymo stebėjimą, reguliarių užprogramuotų klavišų patikrinimą, talkinimą kitiems darbuotojams, kilus problemoms dėl aparato. Nedarbo valandomis aparatus rekomenduojama atjungti.

Telefono automatinio atsakiklio aparatų priežiūra. Naudojantis nuotoliniu automatinio atsakikliu, būtini apsauginiai dažnai keičiami kodai. Patartina nepalikti slaptų įrašų atmintyje, reguliariai klausytis ir šalinti pranešimus, sekti, kad nebūtų perpildyta atmintis.

PBX priežiūra. Visus vartotojus reikia supažindinti su PBX vartojimo instrukcija, standartinių gedimų požymiais bei priemonėms jiems pašalinti. Saugumo sumetimais rekomenduojama pašalinti PBX nuotolinį valdymą. Prieš įsigyjant PBX aparatūrą patartina susirasti ekspertus, galinčius nedelsiant pašalinti gedimus.

Modemų priežiūra. Modemų priežiūra turi aprėpti tokias operacijas: prisiskambinimo numerio įslaptinimas, teisių į tinklinius modemus ribojimas, konfigūracija ir su modemu susijusi programinė įranga nuolat tikrinama, modemas automatiškai išsijungia baigus juo naudotis, o taip pat sekti veiklos duomenis, tikrinti, ar nebuvo bandoma atspėti slaptažodį, įsiregistravimo atveju vartotojui nusiūsti tiksliai patvirtinimą, gaunamiems ir išsiunčiamiems skambučiams turėtų būti skirtos atskiros linijos.

2.2.2. Personalas [Atgal į turinį](#)

Bendras instruktažas. Instruktažai organizuojami, priimant naujus darbuotojus arba prieš pradėdant naudoti naujus programinius paketus ar esant žymiems IS pakeitimams. Instruktuojama pagal vidaus darbo tvarkos taisykles. Reikia motyvuoti reikalavimą nuolat laikytis apsaugos priemonių. Supažindinant turėtų būti aptartas apsaugos supratimas, priemonės susijusios su personalu, priemonės, siejamos su technine ir programine įranga, priemonės aptikus kompiuterinį virusą, naudojimąsi slaptažodžiais, duomenų saugojimas, asmeninių duomenų priežiūra, priemonių pavojaus atveju apžvalga, priemonės, neleidžiančios atskleisti viešai neskelbtinos arba slaptos informacijos, apsaugos priemonių naudojimas. Darbuotojai, tvarkantys, teikiantys ar naudojantys asmens duomenis, privalo pasirašyti pasižadėjimus saugoti asmens duomenų paslaptį.

Darbo aplinkos gerinimas. Bendri patarimai mikroklimato gerinimui – viršvalandžių vengimas, darbo pertraukos, aiškus pareigų paskirstymas, vienodas darbo krūvis, užmokestis, atitinkantis darbuotojo pastangas ir rezultatus, ergonomiškos darbo vietos sukūrimas.

Darbo vietų užpildymas. Dėl planuoto arba neplanuoto neatvykimo į darbą atsiranda laisvų darbo vietų. Patartina iš anksto numatyti, kas atliks laikinąsias pareigas. Naudinga patvirtinti dokumentu esamas darbo vietas bei galimą personalo rotaciją, numatant laikinojo darbuotojo teises ir pareigas. Jei organizacijoje nerandama tinkamo darbuotojo, patartina rasti atsarginį

asmenį iš kitos institucijos, kurį būtų įmanoma pasikviesti laikinai. Prieš atleidžiant darbuotoją, užimsias jo vietą asmuo turi būti informuotas apie būsimąsias pagrindines funkcijas. Verta turėti bendras taisykles, nustatančias, ką turėtų atlikti darbuotojas prieš išeidamas iš darbo. Nauji darbuotojai turi būti supažindinti su organizacijos apsaugos sistema, priemonėmis bei jų naudojimu.

IS administratorius. Administratorius turi išimtinės teises naudotis visomis IS galimybėmis, todėl reikia kruopščiai pasirinkti IS administratorių bei nustatyti jo teisių ribą. Administratorius turi gebėti savarankiškai atlikti kasdieninius IS (įskaitant PBX) valdymo darbus, aptikti ir panaikinti smulkius gedimus, rūpintis duomenų saugojimu. Dažniausiai jis paskiriamas ir duomenų apsaugos įgaliotiniu.

Darbuotojų supažindinimas su telekomunikacinėmis priemonėmis. Darbuotojai turėtų žinoti tokius PBX pranešimus: balsinis ir nuotolinis skambinimas, automatiškas perskambinimas, konferencinis skambutis, linijos užimtumas. Personalui būtina pranešti apie galimus skaitmeninio PBX telefoninio ryšio sutrikimus. Personalas turi būti supažindintas su fakso, telefono automatinio atsakiklio bei modemo naudojimo taisyklėmis ir jų laikytis.

Lygiateisių mazgų tinklų saugos funkcijų taisyklingas naudojimas. Naudojant lygiateisių mazgų tinklą Windows 95 ir WfW terpėse, kiekvienas vartotojas turi rūpintis savo tvarkomų, teikiamų ir naudojamų duomenų apsauga.

2.2.3. Netikėtumų planavimas [Atgal į turinį](#)

Reikalavimų tyrimas. IS grandžių įtaka organizacijos darbui turi būti analizuojama. Reikia atlikti tyrimą IS grandžių ir operacijų svarbai nustatyti. To rezultatas - atskirų operacijų maksimalus toleruotinos prastovos laikas. Pagal tai būtų galima sukurti apsaugos sistemos struktūrą, galimų alternatyvų organizacijos viduje sąrašą. Jei viduje resursų nepakanka, IS grandis reikia importuoti iš išorės. Galimas tiek automatiškas, tiek mechaninis naujos linijos įjungimas esant pagrindinio kelio apkrovai.

“Pavojaus” situacija. Duomenų apsaugos priemonių reikalavimuose aprašant veiksmus pavojaus atveju, reikia apibūdinti visas priemones, kurių būtų imtasi pavojaus atveju (įspėjimas, šalinimo priemonės, grandžių atkūrimo planas). Būtina skirti darbuotojus, kurie būtų atsakingi už pavojaus situacijos nustatymą, pradėtų įgyvendinti numatytus veiksmus. Pareigos turi būti patvirtintos organizacijos vadovybės parašu. Skirtingiems pavojaus scenarijams kuriami skirtingi veiksmų planai, gali būti rengiamos pavojaus situacijos pratybos, rezultatai - fiksuojami dokumentiškai. Pavojaus pasekmėms sušvelninti galimas trejopas draudimas: turto, pasekmių bei personalo.

IS atsarginių dalių įsigijimo planavimas. Siekiant pagreitinoti šį procesą, patogų remtis tokiais dokumentais: grandies tikslus apibūdinimas, gamintojas, tiekėjas, pristatymo laikas, įjungimo laikas. Sąrašą reikia nuolat papildyti. Svarbu, kad sutartis dėl galimybės įsigyti atsarginių dalių galiotų ir pasibaigus garantiniam aptarnavimo laikui.

Kompiuteriniai virusai. Reikia turėti atsarginį diskelį su operacine sistema, iš kurio, kilus nesklandumams, galima būtų pradėti darbą. Diskelyje dar turėtų būti redaktorius, atsarginių kopijų kūrimo programa. Panaikinus virusą, pažeistas bylas reikia pabandyti atkurti iš atsarginių kopijų archyvo.

Duomenų saugumas. Į duomenų apsaugos reikalavimus rekomenduojama įtraukti duomenų saugojimo tvarką. Kuriant duomenų apsaugos koncepciją, verta pasinaudoti šia struktūra: apibrėžimai, motyvuojamieji rizikos veiksniai, IS veikiantys faktoriai, IS duomenų apsaugos planas, minimali duomenų apsauga, darbuotojų duomenų apsaugos svarbos supratimas, reguliarius bandymai atkurti duomenis. Pagrindiniai duomenų išsaugojimo tipai: duomenų dubliavimas, pilnas duomenų perrašymas, dalinis duomenų perrašymas, diferencinis duomenų perrašymas. Organizacijoje turi būti pradėta tvarkyti vienoda išsaugotų duomenų dokumentacija: įrašymo data, struktūra, laikmenos, kuriose operaciniai ir išsaugoti duomenys laikomi, saugojimo įrenginiai ir programinė įranga bei naudoti parametrai. Saugojimo laikmenos turi atitikti

keliamus reikalavimus – tikslai įgalintiems asmenims suteikiama teisė naudoti laikmenas, turi būti garantuotas pakankamas ryšio greitis, laikmenos turi būti laikomos atskirai nuo kompiuterio.

Windows NT priežiūra. Kiekvienas kompiuteris privalo turėti savo atskirą paleidžiamąjį diskelį, kuris naudojamas, įvykus sistemos sutrikimui. Siekiant sumažinti serverio apkrovą, užtikrinti saugumą, duomenys lygiagrečiai rašomi į kelis kietuosius diskus, įmontuotus serveryje. Windows NT terpėje yra speciali atsarginių kopijų kūrimo programa *ntbackup.exe*.

Windows 95 priežiūra. Išskyla grėsmė dėl ribojamo bylų pavadinimų ilgio (8.3). Kiekvienam kompiuteriui sukuriama (*Control Panel/Software*) atskiras paleidžiamasis diskelis. Norint kiekvienam vartotojui turėti asmeninį diskelį reikia panaudoti *Emergency Recovery Utility* programą iš Windows 95 CD-ROM.

PBX sauga. Įvykus visiškam ar daliniam gedimui, turi būti atskira linija, skirta avariniams pranešimams. PBX turi funkciją, įgalinančią pavojaus atveju linijas persikirstyti iš anksto nustatytiems terminalams. Ši funkcija turi būti aktyviai naudojama.

CMOS RAM apsauga. Visi saugojimo parametrų nustatymai turi būti atlikti mechaniniu įvedimu. Patogiausia pasižymėti atliktus pakitimus arba naudoti specialią programą (galvučių, sektorių ir cilindrų skaičius kietajame diske), registruojančią visus duomenis.

2.3. Techninės ir programinės priemonės [Atgal į turinį](#)

2.3.1. Techninė įranga [Atgal į turinį](#)

Nešiojamųjų kompiuterių apsauga. Naudoti išsiregistravimo slaptažodį, energijos taupymo režimą, duomenų kodavimo programas, nepalikti slaptų duomenų kietajame diske, energijos rezervų stebėjimas - pagrindinės nešiojamųjų kompiuterių apsaugos priemonės.

Apsauga nuo patalpų pasiklausymo. Pasiklausymui naudojamus įtaisus: telefonus automatinis atsakiklius ir kompiuterių mikrofonus, nesinaudojant patariama išjungti.

PBX techninė apsauga. Visi PBX pagalba atliekami valdymo darbai turi būti registruojami ir kaupiami duomenų bazėje arba archyve spausdintoje formoje. Kiekvienas konfigūracijos pakeitimas turi būti patvirtintas dokumentu, o dokumentacija tikrinama. Iš gamintojų gautoje informacinėje technikoje bei PBX yra nustatyti standartiniai slaptažodžiai, kuriuos reikia nedelsiant pakeisti naujais. PBX terminalų slaptažodžių vartojimas apsaugo nuo piktnaudžiavimų telefoniniu ryšiu. PBX įrenginiai, kuriais galima valdyti sistemos veiklą, turi būti rakinami.

Fakso sistemos sauga. Vengiant nepageidaujamų fakso pranešimų, įmanoma blokuoti arba riboti pranešimų gavimą arba gavėjo numerius, be to telefono ryšio tiekėjas gali sukurti uždara grupę, kurioje vartotojai galėtų keistis informacija tik tarpusavy.

2.3.2. Programinė įranga [Atgal į turinį](#)

Garantuota sistemos priežiūra. Sistemos priežiūrą atlieka administratorius. Paprastiems darbams atlikti administratorius turi turėti ir naudoti paprasto vartotojo išsiregistravimo vardą bei slaptažodį. Esant keliems administratoriaus teisės turintiems vartotojams, reikia tinkamai derinti jų veiklą.

Saugūs išsiregistravimai. Išsiregistravimo programa turi būti naudojama, ribojant nesėkmingų bandymų skaičių. Ilgą laiką nenaudojami išsiregistravimai turi būti blokuojami ir ištrinami. Taip pat reikia elgtis ir su nevartojama terminalais. Tikslinga sukurti išsiregistravimo vardus ribotam laikui. Patartina, kad visi sistemos vartotojai, palikdami darbo vietą ilgesniam laikui, informuotų administratorių.

Slaptažodžiai. Slaptažodžiai – patogiausias kelias nustatyti vartotojo teises. Jie gali būti tikrinami įsijungus į IS arba prieš įsijungiant, taip pat naudojami ekranų informacijos apsaugai.

Programinės įrangos apsauga. Naudingiausios programinės įrangos paketų siūlomos apsaugos funkcijos: slaptažodžiu apsaugotas programinės įrangos vartojimas, slaptažodžiu apsaugota galimybė naudoti bylas, automatiškas darbo duomenų kopijavimas, automatiškas bylos pervardinimas ją saugant, duomenų kodavimas. Programinės įrangos turi būti palikta tik tiek, kiek reikalinga efektyviam darbui, likusią patariama išinstaliuoti. Minimalūs reikalavimai saugos produktams DOS terpėje su keletu vartotojų: IS administratoriaus ir vartotojų identifikavimas,

skirtingos valdymo ir stebėjimo teisės, įsiregistravimas, ribojamas paprastųjų vartotojų priėjimas prie operacinės sistemos, ekrano apsauga, neįmanomas sistemos įjungimas iš lanksčiojo diskelio.

Duomenų laikmenų priežiūra. Prieš duomenų kopijavimą informacija laikmenose turi būti ištrinama, prieš ir po duomenų persiuntimo naudojama virusų aptikimo, duomenų tikrinimo ir kodavimo programos. Sumos patikrinimas naudojamas siekiant nustatyti, ar nebuvo manipuluota informacija siuntimo metu, o elektroniniai parašai įrodytų siuntėjo autentiškumą. Patartina naudoti specialias priemones diskelių nuskaitymo įrenginių blokavimui.

Vidinio tinklo apsauga. Apsaugos priemonės turi nustatyti kiekvieno programinio paketo, patenkančio į vidinį tinklą ir išsiunčiamo iš vidinio tinklo, IP numerį, laiką, datą bei paslaugą. Galimi paketų veiklos ribojimai – nuo pirmumo teisių suteikimo iki tam tikrų ryšių uždraudimo. Sugedus apsauginiams filtrams, sistema turi būti sustabdyta.

UNIX apsauga. UNIX terpėje pagal identifikavimo kodą nustatomos vartotojų teisės, galima sekti jų veiklą. Identifikavimo kodas turi būti naudojamas vieno vartotojo ar vartotojų grupės. UNIX terpėje tik įvedus teisingą kliento vardą, įsiregistravimas tęsiamas tikrinant slaptažodį. Slaptažodžiai neturi būti laikomi bendrai prieinamoje byloje, jie saugotini tik vienam vartotojui skaitomoje byloje. Įsiregistravimo bylos turi būti nuolat tikrinamos. UNIX serverio apsaugos priemonės – BIOS slaptažodis, ypatingo vartotojo slaptažodis kompiuterio perkrovimui, klaviatūros užraktai. Sisteminės bylos bei katalogai turi būti pasiekiami tik administratoriaus teises turintiems vartotojams (*t-bit* katalogai prieinami visiems vartotojams, *s-bit* tiktai sistemos administratoriams). Vartotojas turi turėti pakankamai teisių, kad galėtų apsaugoti savo bylas nuo kitų vartotojų. Žymėjimas *s-bit* turi būti naudojamas tiktai pasikonsultavus su administratoriumi bei pagrindus priežastis. Vartotojas, naudodamasis ypatingo vartotojo byla, įgyja administratoriaus teises, todėl tik būtiniausios bylos gali turėti ypatingas teises. UNIX terpėje vartojant tam tikras komandas, įmanoma gauti duomenų apie visus vartotojus, todėl reikia riboti vartotojų, besinaudojančių šiomis komandomis, skaičių.

Windows 95 ir WfW apsauga. Windows terpė turi mažai apsaugos priemonių, todėl ją naudoti patartina tik saugioje aplinkoje. Turi būti griežtai reguliuojamos vartotojų teisės, atsisakoma universalių teisių. Pageidautina, kad įsiregistravimo metu sukurtas slaptažodis būtų naudojamas ryšio tarp lokalinio tinklo ir kliento identifikavimui. Siunčiamas slaptažodis turi būti koduojamas. Naujasis WfW ir Windows 95 vartotojas turi galimybę sukurti slaptažodžių sąrašą (*[vartotojo vardas].pwl*). Sąraše bus registruojami visi naudoti slaptažodžiai. WfW įsiregistravimo slaptažodis daugiausia skirtas šiam sąrašui apsaugoti. Įsiregistravimo slaptažodis nebūtinai, kai kompiuteris turi vieną vartotoją ir veiksnius kitos saugos priemonės. Windows 95 pašalintos bylos perkeliama į šiukšlių dėžę (*Recycle Bin*). Šalinant slaptų duomenų bylas, patartina jas neatpažįstamai pakeisti.

Windows NT apsauga. Windows NT terpėje kiekvienas vartotojas privalo turėti savo slaptažodį. Windows NT dirba saugiai, jeigu nuo pat pradžios sukuriama uždara, apsaugota darbo aplinka. Windows NT instaliacijos metu derėtų pasirinkti: saugią versiją (turi būti 3.51 arba naujesnė), bylų sistemą (instaliavimo metu reikia formatuoti *NTFS* sistema), įsiregistravimo konfigūraciją, pagalbines terpes, papildomas (nestandardines) paslaugas, įrangos apsaugą, pagalbinį disko taisymą, apibrėžtųjų vartotojų registrą, įjungimą į tinklą.

2.4. Telekomunikacinės priemonės [Atgal į turinį](#)

2.4.1. Techninė įranga [Atgal į turinį](#)

Serverio priežiūra. Teisės naudotis serverio kietuoju disku turi būti ribojamos. Jeigu tinklo serverio disko atmintis ribota, vartotojams turi būti nustatyta maksimali saugomų duomenų kiekio riba. Įvedimo įrenginys turi būti blokuotas. Įsiregistravimas į serverį turėtų būti ribotas. Reikia nuolat stebėti įsiregistravimo bylas, dėmesį atkreipiant į klaidingus slaptažodžio įvedimus, į teisingą vartotojo identifikavimo kodą, bandymus pažeisti teisių ribojimus, ryšio nutrūkimus, tinklo perkrovą.

Kabeliai. Tipų pasirinkimas priklauso nuo atstumo bei duomenų persiuntimo spartos. Dokumentuose turi būti išsamūs, reguliariai atnaujinami duomenys: kabelio tipas, žymėjimas,

išskirstytojų vietas, tikslus kabelio išdėstymas patalpose, linijų išmatavimai, vartotojai, jungties taškų techniniai rodikliai, rizikos veiksniai, įdiegtos saugos priemonės. Šią informaciją patartina padalinti į kelias dalis ir laikyti saugiai. Kabeliai tiesiami taip, kad jie būtų prieinami tiktai vartotojams ir kartu apsaugoti nuo tiesioginių mechaninių pažeidimų. Patartina pašalinti nenaudojamas linijas ir blokuoti nenaudojamas jungtis.

Faksogramų siuntimas. Tituliniame lape gali būti nurodyta tokia informacija: adresatas bei jo duomenys (fakso ir telefono numeris, adresas), siuntėjo vardas bei jo duomenys, asmuo kontaktui esant siuntimo nesklandumams, puslapių skaičius, dokumento svarba, siuntėjo parašas. Siuntimo ir priėmimo duomenys turi būti reguliariai išspausdinami ir saugomi sutartą laiką, patartina tikrinti fakso numerius. Šioms užduotims atlikti skiriamas darbuotojas. Perduodant ar gavus svarbią faksogramą patartina perspėti suinteresuotas puses. Fakso aparatu įmanoma užprogramuoti dažnai renkamus numerius, tačiau juos reikia reguliariai tikrinti.

Modemas. Modemo konfigūracija turi būti patvirtinta dokumentu ir saugoma atskirai nuo aparato. Pagrindinės saugos priemonės: automatinis atsakymas, nuotolinis modemo konfigūracijos nustatymas, slaptažodžiu apsaugotas perskambinimo numerių sąrašas ir programinė įranga, vienos krypties ryšys. Pagalbinės saugos priemonės: po nesėkmingo bandymo naudojama laiko uždelsimo funkcija, priežiūros personalo teisių ribojimas, tvarkymo darbų nutraukimas standartinių operacijų metu, jeigu taisymo darbus atlieka ne organizacijos darbuotojai, jų veikla turi būti stebima organizacijos IS administratoriaus.

2.4.2. Programinė įranga [Atgal į turinį](#)

Tinklo valdymas. Tiesiamiesiems tinklams išdėstyti galima pasirinkti keturis variantus: *star* (visi vartotojai savo kabeliais prisijungę prie centrinio išėjimo), *tree* (klientai prisijungę prie tinklo mazgų, kurie savo jungtimis jungiami prie išėjimo), *bus* (visi vartotojai sujungti į bendrą liniją) ir *ring* (tai *bus* tipo tinklas, kurio galai yra sujungti). Tiesiant daugiau tinklų, juos reikėtų segmentuoti – tiesiti po keletą tinklų, sujungtų į vieną sistemą. Organizacijos tinklo valdymas turi būti centrinis. Centrinis turi būti ir kabelių pasirinkimas ir planavimas, IS įrenginių ir programinės įrangos pasirinkimas, tinklo adresų bei vartotojų identifikavimo kodų paskirstymas, tinklo dalių paskirstymas organizacijos struktūrinėms dalims. Kiekvienam vietinio tinklo vartotojui turi būti suteiktas slaptažodis, kuris papildomai saugomas užklijuotame voke ir naudojamas tik patvirtintus dokumentu. Tinklo patikrinimas turi būti vykdomas bent kartą per mėnesį. Reikia atkreipti dėmesį į vartotojus: be slaptažodžių; nesinaudojančius IS paslaugomis; į tuos, kurių slaptažodžiai neatitinka organizacijos keliamų reikalavimų; į turinčius teises, lygias administratoriaus teisėms. Turi būti skirtas atsarginis administratorius, kuris galėtų užimti pagrindinio pareigas.

Nuotolinio ryšio apsauga. Svarbiausia apsaugos užduotis – nustatyti ir užkirsti kelią bandymams iš išorės prasiskverbti į vidinį tinklą. Siekiant apsaugoti vidinį ryšį per modemą, nedera viešai atskleisti modemo telefono numerio, patariama sukurti uždaras vartotojų grupes, būtinas automatiškas perskambinimas, ryšio tinklo teisių ribojimas, identifikavimas. Saugiausia būtų atsisakyti išorinio nuotolinio ryšio, tačiau tokio prireikus, yra keletas apsaugos priemonių, sustiprinančių patikimumą: kompiuterio vartų naudojimas tarp modemo ir ryšio mazgo, išorinio nuotolinio ryšio mazgo išjungimas jo nenaudojant, uždarų vartotojų grupių kūrimas, tiesioginio prisiskambinimo kontrolė.

NFS ir NIS apsaugos mechanizmas. NFS suteikia galimybę visiems tinklo kompiuteriams naudotis bylomis, esančiomis serveryje. Todėl vartotojams reikia suteikti kuo mažiau teisių, o sisteminėmis bylomis leisti naudotis tiktai administratoriui, naudoti *Secure NFS*, kuris siunčia koduotus duomenis. NIS yra lengvai pažeidžiamas, todėl turi būti naudojamas tiktai saugioje aplinkoje. Svarbu taip nustatyti teisingą slaptažodžių atpažinimo režimą serveryje, kad jis atsilieptų tiktai į iš anksto pažymėto kompiuterio paklausimą.

Duomenų siuntimas. Duomenų siuntimas priklauso nuo galimų rizikos veiksnių, duomenų slaptumo bei skiriamo tam laiko. Elektroninio pašto siuntimas - viena dažniausiai naudojamų tinklo paslaugų. Patariama naudoti naujausias programinės įrangos versijas. Kad duomenys būtų

perduodami sėkmingai, turi būti suderintos siuntimo/priėmimo sistemos, naudojamas duomenų kodavimas.

Kodavimas. Vartotojas turi nusprėsti, ar naudotis pranešimų kodavimo, ar skaitmeninio parašo apsauga. Tinklams, kuriuose nėra vykdomas kodavimas, patartina naudoti trumpalaikius slaptažodžius.

Saugumas, naudojant Internetą. Naršant WWW gali kilti saugumo problemų dėl klaidingų vartotojo veiksmų, netinkamos naršyklės konfigūracijos arba trūkstamų saugumo priemonių. Patartina naudotis šiomis saugos priemonėmis: programų saugumas (pradžioj programa turi būti išbandyta atskirtu nuo tinklo kompiuteriu); bylų, kuriose saugomas WWW tiekėjų sukurtas vartotojo profilis, priežiūra; vartotojų ryšio su Internetu dokumentacijos saugojimas; teisių į vartotojo kietąjį diską ribojimas; informacijos kodavimas; duomenų apie saugos spragas kaupimas; organizacijos nustatytų taisyklių laikymasis. Siekiant sumažinti Interneto keliamą riziką vietiniam tinklui, prie išorinio tinklo prijungtą kompiuterį yra tikslinga atskirti nuo organizacijos sistemos.

UNIX tinklas. UNIX sistemoje svarbu neleisti neteisėtiems vartotojams naudotis kompiuteriu, uždrausti diskelių nuskaitymo įrenginį, taikyti ribojimus veiksams su UNIX sisteminiemis bylomis. Jungiant kompiuterius į UNIX tinklą per NFS, reikia nustatyti jų teises į bylas bei katalogus, riboti pagrindinių teisių teikimą, kontroliuoti parametru nustatymą, bylas kopijuojant į UNIX. Keičiantis duomenų laikmenomis būtina saugotis, kad į UNIX sistemą nepatektų ir neišplistų virusai. UUCP teikia dviejų IS duomenų apsikeitimo ir nuotolinio valdymo galimybę. Naudojant šią programinę įrangą, reikia pašalinti įrangos bei susijusių bylų konfigūracijos skirtumus, kiekvienai IS sukurti atskirą vartotojo identifikavimo kodą bei slaptažodį, stebėti slaptažodžius, nes jie yra nekoduojami. Naudojant UUCP yra sukuriami protokolai, kurie turi duomenų apie visas operacijas. Protokolai turi būti reguliariai tikrinami ir įvertinami.

Windows tinklai. Naudojant RAS, galima prisijungti prie Windows NT sistemos, lyg dirbant vietiniu tinklu. Darbo saugumą lemia pasirinktos kodavimo programos. RAS leidžia naudoti papildomą saugumą garantuojantį įrenginį – kompiuterį su periferine įranga, tikrinančia identifikavimo korteles. Taip pat galima perskambinimo funkcija, administratorius gali stebėti, kokie tinkle esantys informacijos resursai yra pasiekiami prisijungusio vartotojo. Svarbi saugumo stiprinimo detalė – teisingos Windows NT konfigūracijos pasirinkimas. Naudojant WfW, Windows 95 ir NT, šalia serverio palaikomo vietinio tinklo, gali būti įrengtas lygiateisių mazgų tinklas. Toks dvigubas tinklas yra nepatartinas.

[Atgal į turinį](#)

XXXXX